

EXHIBIT 1

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of VermontU.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

2023 AUG -9 PM 5:31

CLEAR

BY

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)81 BERLIN STREET, APARTMENT 2,
MONTPELIER, VT

Case No. 2:23-mj-098

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____ Vermont _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2251	Production of CSAM
18 U.S.C. §§ 2252	Distribution of CSAM
18 U.S.C. §§ 2252A	Possession of CSAM

The application is based on these facts:

See attached Affidavit.

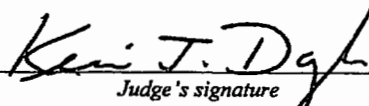
☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Josh Otey, Special Agent HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: August 9, 2023



Judge's signature

City and state: Burlington, Vermont

Honorable Kevin J. Doyle, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is 81 Berlin Street, Apartment 2, Montpelier, Vermont. 81 Berlin St. is a two-story grey building with three apartment units. The Subject Premises is an apartment within the building having an entry at the rear of the 2nd floor of the building. Apartment 2 is the only apartment accessed from the rear of the building. 81 Berlin St. is shown in the following image taken on or about August 9, 2023:



ATTACHMENT B

I. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offense

The items to be seized from the Subject Premises are the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2251 (production of child pornography), 2252(a)(2) & 2252A(a)(2) (receipt of child pornography), and 2252(a)(4) & 2252A(a)(5) (possession of child pornography) (the "Subject Offense"):

1. Computer devices, storage media, cellular telephones, and related electronic equipment used to access, transmit, or store information relating to the Subject Offense;
2. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
3. Books and magazines containing visual or written depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
4. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
5. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
6. Correspondence and records pertaining to violation of the Subject Offense including, but not limited to envelopes, letters, mailings, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
7. Records evidencing occupancy or ownership of the Subject Premises, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence;
8. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the Subject Offense, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
9. Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
10. Any child pornography as defined by 18 U.S.C. § 2256(8);

11. Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
12. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
13. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
14. Mailing lists, supplier lists, and mailing address labels related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
15. Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises include any computer devices, storage media, and related electronic equipment that may contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offense falling within the categories set forth in Section I.A above. In lieu of seizing any such computer devices, storage media, and related electronic equipment, this warrant also authorizes their copying for later review.

To facilitate this review, the items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any records or other items which evidence ownership, control, or use of, or access to any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

Any materials seized under this Section II.B that are later determined not to contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offense falling within the categories set forth in Section II.A above will be returned to the Subject Premises within 60 days of their seizure.

C. Use of Fingerprints and Face

During the execution of this search warrant, law enforcement personnel are authorized to press the fingers (including thumbs) of COOLIDGE to the fingerprint sensor of any smartphones seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. During the execution of this search warrant, law enforcement personnel are authorized to have COOLIDGE remain still and look, with eyes open, at the camera of any smartphones seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Joshua Otey, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with Homeland Security Investigations, Department of Homeland Security ("HSI"), currently assigned to HSI's Burlington Office. I have been a Special Agent with HSI since March 2020. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have participated in a number of investigations into the receipt, possession, and/or distribution of child pornography by electronic means. I have gained expertise in these areas through training and daily work related to conducting these types of investigations. I also have experience executing search warrants, including search warrants for physical premises and electronic evidence.

2. I have personally participated in the investigation of the offense discussed below. I am familiar with the facts and circumstances of this investigation from my participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography.

3. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below, further described in Attachment A, for the items and information described in Attachment B. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of computers and electronically

stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

A. The Subject Premises

4. The premises to be searched (the “Subject Premises”) is 81 Berlin St., Apartment 2, Montpelier, Vermont. 81 Berlin St. is a two-story building with multiple apartments. The Subject Premises is an apartment within the building that has an entry on the 2nd floor of the building. The Subject Premises is described in more detail in Attachment A to this application.

B. The Subject Offenses

5. For the reasons detailed below, I submit that there is probable cause to believe that the Subject Premises contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251 (production of child pornography), 2252(a)(2) & 2252A(a)(2) (distribution of child pornography), and 2252(a)(4) & 2252A(a)(5) (possession of child pornography) (the “Subject Offenses”), as described in Attachment B.

C. Terminology

6. As used herein, the following terms have the following meaning:

a. Child Pornography: defined in Title 18, United States Code, Section 2256(8) in pertinent part as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct”

b. Computer: includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

c. Computer hardware: all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices) and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. Computer software: digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. Computer Data/ESI (Electronically Stored Information): consistent with Fed. R. Crim. P. 41 and the Advisory Committee Comments to the 2009 amendments, ESI includes writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, including all types of computer-based information as may be developed over time. "Computer data" as used herein is synonymous with ESI.

f. Computer Passwords, Pass-Phrases, and Data Security Devices: as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. Directory or Folder: a simulated electronic file folder or container used to organize files and directories in a hierarchical or tree-like structure.

h. File: a collection of related data or information stored as a unit under a specified name on storage medium. Not all ESI is stored in files.

i. File Extension: many operating systems allow a filename extension that consists of one or more characters following the proper filename. For example, image files are frequently stored as .bmp, .gif, .jpg, or .tiff; audio files commonly come in a variety of formats such as .aud, .wav, or .mp3. The filename extension should indicate the file type or format; however, users may change filename extensions to evade firewall restrictions or for other reasons.

Accordingly, file types must be identified at a binary level or by viewing the contents of the file, rather than by relying on file extensions alone.

j. Forensic Copy/Image Copy: a data compilation created with the use of forensic software that contains an exact copy, sometimes referred to as a bit-by-bit copy, of an entire physical storage medium (hard drive, smart phone, DVD, tape, etc.), including all active and residual data and unallocated or slack space on the media. Forensic copies are sometimes called “images” or “imaged copies” or “mirror images.” Forensic copies are generally only reviewable via forensic review software (meaning that user files contained within a forensic copy cannot simply be opened with the program originally used to create them). User files can, as useful, be extracted from forensic copies for ease of review; but review of latent or residual data, where needed, must generally take place via forensic review software.

k. Internet: a global network of computers and other devices that communicate with each other. It supports services such as email, the World Wide Web, file transfer, and Internet Relay Chat. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when devices communicating with each other are in the same state.

l. Internet Protocol address (“IP Address”): a unique numeric address used to identify a particular computer connected to the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

m. Latent/Residual Data: deleted files and other ESI that are inaccessible without specialized forensic tools and techniques. Until overwritten, this data resides on media such as a hard drives in unused space and other areas available for data storage. It can include data within files that has functionally been “deleted” in that it is not visible using the application with which the file was created absent use of undelete or special data recovery techniques.

n. Metadata: data that describes characteristics of other ESI, for example, how, when, and by whom that ESI was collected, created, accessed, modified, and formatted. Metadata can be found in different places in different forms; it can be created by applications, users, or the file system; and can be altered intentionally or inadvertently. Some metadata, such as file dates and sizes, may be easily accessible; other metadata can be hidden or embedded and unavailable without technical skill and tools.

o. Records, documents, and materials: include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic

or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

p. Slack Space: space within a cluster (unit of storage space for a file) that is not being used for storage of the file, but which may contain latent or residual data relating to the file or to other activity on the computer.

q. Storage Medium, ESI Storage Device, ESI Storage Media, Electronic Storage Media: any device or physical object capable of storing ESI, including computers, optical disks such as CDs and DVDs, RAM (random access memory), floppy disks, flash memory, thumb or flash or USB drives, tapes and cartridges, and other magnetic or optical media.

r. User File: a file generated by a user, generally by using a program or application such as a word processor or photo editor, as distinct from files constituting, or generated by, the system or program.

s. “Minor,” “Sexually Explicit Conduct” and “Visual Depiction”: are defined as set forth in Title 18, United States Code, Section 2256.

II. Probable Cause

7. Through investigative research and through conversations with other individuals, I have become familiar with the Tor network, otherwise known as the darkweb. The Tor network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user’s web browser or by downloading the free “Tor browser bundle” available at www.torproject.org. Use of the Tor software bounces a user’s communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor “exit node,” rather than the user’s actual IP address, shows up in the website’s IP log. An exit node is the last computer through which a user’s communications were routed. There is

no practical way to trace the user's actual IP address back through that Tor exit node IP address. A criminal suspect's use of Tor accordingly makes it extremely difficult for law enforcement agents who are investigating a Tor "hidden service" to detect the host's, administrator's, or users' actual IP addresses or physical locations.

8. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services" operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dfiku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

9. The HSI Office in Portland, Maine, has an ongoing investigation to identify victims of child sexual abuse ("CSE") on the darkweb, as well as locate those individuals committing such crimes against children. HSI Portland works to accomplish this mission by infiltrating and dismantling criminal organizations that operate CSE forums and chat sites on the darkweb. Additionally, HSI Portland works with and coordinates with law enforcement partners both domestically and internationally to achieve these goals. HSI Portland seeks to identify the individuals committing these crimes on the darkweb utilizing encrypted applications to include but not limited to Telegram, Session, ICQ, WhatsApp, and Signal.

10. In or about January 2022, an individual using the screenname “phantasy” made a post on a darkweb site dedicated to the sexual abuse of children stating “*Would anyone please have pics or gifs of lil boys having there [sic] rectal temperatures taken? Thank you.*”

11. On January 5, 2022, an HSI Portland undercover agent participated in a conversation with the individual using the screenname “phantasy” on a separate darkweb site dedicated to the sexual abuse of children, on which likeminded individuals discuss the sexual abuse of children. Since that conversation, law enforcement has been attempting to identify user phantasy (hereinafter “PHANTASY”).

12. Throughout the investigation, image and video files posted to a darkweb site under investigation (the Subject Site), which were publicly available to any registered user at the time of posting, were captured and archived for law enforcement review.

13. As of August 2023, PHANTASY had posted over 38,300 messages and distributed over 8,000 images or videos of sexually explicit depictions of children on the Subject Site. Some of those 8,000 files match images that have previously been identified as child sexual abuse material and documented as such by the National Center for Missing and Exploited Children.

14. On August 8, 2023, PHANTASY was logged into the Subject Site and made statements to include the following:

14:12 EST – hello family, im back and on cloud nine! OMG

14:16 EST – I just spent an hour w/ my lil bf here alone. He is so adorable! And.....

14:25 EST – close! I got to take his rectal temp and....

14:27 EST – I asked him if it felt good and he said yes.....

14:29 EST – he was semi hard [drooling emoji]: I had to give him “medicine” in his butt to make sure he want sick....i used my pinky...

15. On August 8, 2023, at approximately 19:29 EST, in the course of a private conversation with an undercover officer on the Subject Site, PHANTASY distributed a series of four images on the Subject Site. Three of the images depict a young boy full clothed in the same outfit. One of those three also depicts a young girl who resembles the boy. The fourth image, `Img_3197.jpg`, depicts a young boy's buttocks with a thermometer protruding from them. The boy is leaning against a gray couch and has a red shirt on. The focus of the image is the buttocks and thermometer, but the boy's skin complexion and shirt color are consistent with the skin complexion and shirt color of the boy depicted in the other three images. I have reviewed the four images.

16. In conversations both public and private on the Subject Site, PHANTASY described his interactions with an Indian family who lived downstairs from him and stated that he had access to the children of that family and that he was alone with those children on occasion. PHANTASY further described sexually abusing the male child of that family.

17. Through the course of conversations with other participants on the Subject Site as well as with undercover agents, PHANTASY has discussed their fetish of using/seeing rectal thermometers used to penetrate children's anuses.

18. HSI Portland agents reviewed a different darkweb site that had been seized by law enforcement. The other site included information about the passwords used by some of the site's members. One of those users used the moniker "phantasy." HSI maintains a database of hundreds of thousands of usernames operating on the darkweb. Of those hundreds of thousands of usernames, only one is "phantasy," with that capitalization style and spelling. There is no other username of phantasy with other capitalization in the database. The usernames in this database are case-specific. I know from my training and experience that users of darkweb sites dedicated to the sexual abuse of children use the same monikers, or usernames, across darkweb sites. Doing

so enables those users to build trust with each other and find each other on different sites. Based on my training and experience and the appearance of the username “phantasy” on this other darkweb site and in the HSI database, I believe this “phantasy” to be the same PHANTASY under investigation. From this other darkweb site, HSI Portland agents were able to determine PHANTASY’s password to be “jcool3665.”

19. A query of Vermont Law Enforcement records revealed that Jeffery Paul COOLIDGE, who resides at 81 Berlin Street, Apartment 2, Montpelier, Vermont, has a date of birth (DOB) of 03-06-1965. PHANTASY’s password of “jcool3665” matches a compilation of Jeffery Paul COOLIDGE’s first initial, first four letters of his last name, and the digits of his date of birth.

20. Law enforcement records document previous Vermont Sex Offender Registry checks of COOLIDGE as recently as 2017, meaning that COOLIDGE was listed on the sex offender registry at least up until that year. COOLIDGE is no longer listed as an active registrant on the Vermont Sex Offender Registry.

21. Jeffery Paul COOLIDGE has a criminal history in the State of Vermont that includes a 1997 arrest and conviction for Lewd and Lascivious Conduct with a child and Sexual Assault.

22. On August 9, 2023, HSI Burlington agents met with Montpelier Police Detectives (“MPD”) to discuss COOLIDGE. HSI agents learned that MPD is familiar with COOLIDGE and interact with him on a regular basis. They were also aware of COOLIDGE’s residential address and that it is situated upstairs from the residence of an Indian family with young children.

23. On August 9, 2023, HSI Burlington Agents conducted surveillance at COOLIDGE’s residence, 81 Berlin Street, Montpelier, Vermont. At approximately 12:15 EST,

HSI Burlington agents met with the landlord for the residence located at 81 Berlin Street, Montpelier, Vermont. The landlord informed the agents that the tenants of the residence include Jeffery COOLIDGE, who occupies a second-floor efficiency style apartment labeled as Apartment 2. Additionally, the landlord confirmed that a family from India occupies a downstairs apartment within the building and has a minor male and minor female child. The landlord stated that he is familiar with the family and children and had purchased them a bicycle on a previous occasion. The landlord was shown one of the four images described above, that PHANTASY posted to the Subject Site, that depicts both the minor boy and girl fully clothed. The landlord immediately recognized the depicted children and confirmed they are the children who lives in the downstairs apartment.

24. The landlord further stated that has been inside Apartment 2 and observed COOLIDGE in the apartment. The landlord stated that COOLIDGE is regularly on his computer when in his apartment.

25. Based on my training, experience, and conversations that I have had with other federal agents and law enforcement officers, I have learned the following:

a. Child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography usually do so by ordering it from abroad or through discreet contacts, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic communications conversing with other collectors in order to solicit and receive child pornography.

b. I know that people who collect and trade child pornography typically do not destroy or delete image files or video files depicting child pornography. Instead, collectors of

child pornography typically retain their materials and related information for many years, and sometimes indefinitely. Even when files are deleted from a computer, they can frequently be recovered during a forensic examination.

c. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. Such individuals in possession of files containing child pornography are likely to save and maintain these files on their computers or other portable storage devices so they are readily accessible in their home, office, or vehicle.

d. Because of the illegality and the severe social stigma child pornography images carry, these individuals hide them in secure places. These secure physical places often include physical places such as the home or other structures on the property where the individual resides. These secure physical places can also include secure electronic places such as hidden files on the hard drives of the individual's computers, external storage media, including but not limited to cellular phones or thumb drives.

e. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers, and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

f. I am also aware that an individual who possesses more than one computer or smart phone may send a file containing child pornography from one phone to another phone or from one laptop to another in order to maintain, preserve and/or hide the file.

26. In light of the foregoing, information in support of probable cause in child pornography cases is unlikely to be stale because collectors and traders of child pornography are

known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

27. Based on my training and experience, I know that persons who collect and distribute child pornography frequently collect and view sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. These examples of visual media containing sexually explicit materials are often times stored on various devices, including but not limited to, computers, disk drives, modems, thumb drives, personal digital assistants, mobile phones and smart phones, digital cameras, and scanners, and the data within the aforesaid objects relating to said materials.

28. Based on the foregoing, I respectfully submit that there is probable cause to believe that COOLIDGE, who lives at the Subject Premises, is engaged in the commission of the Subject Offenses, and that evidence related to the Subject Offenses may be found at the Subject Premises and within and upon computers, cellphones, electronic storage media, and other electronic devices capable of storing data, information, and images.

29. Individuals who engage in the criminal activity described herein, in the event that they change computers, will often back up or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, which would be valuable in facilitating their criminal activity. In addition, individuals who engage in such criminal activity will often also store or transfer files on electronic storage media other than computer hard drives, including thumb drives, flash memory cards, CD-ROMs, or portable hard drives to, for example, facilitate the use of the information or to transfer it to co-conspirators in support of the criminal scheme.

30. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files can be stored on a hard drive for years at little or no cost. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. Specifically, when a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Deleted files, or remnants of deleted files, may accordingly reside in “slack space” for long periods of time before they are overwritten. In addition, a computer’s operating system may keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are generally automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

31. Based on the foregoing, I respectfully submit there is probable cause to believe that evidence of COOLIDGE’s commission of the Subject Offenses is likely to be found in ESI recovered from the Subject Premises.

III. Procedures for Searching ESI

32. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport

them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

33. The seized devices may include smartphones that offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) or facial recognition in lieu of a numeric or alphanumeric passcode or password. For Apple devices, for example, this feature is called Touch ID or Face ID, depending on the model of the Apple device.

34. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) found at the bottom center of the front of the device. Similarly, Face ID allows a user to unlock the iPhone X and later models. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user’s face. Face ID confirms attention by detecting the direction of the user’s gaze, then uses neural networks for

matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user's appearance, and carefully safeguards the privacy and security of the user's biometric data.

35. In my training and experience, users of mobile devices that offer security technology like Touch ID and Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

36. In some circumstances, a fingerprint cannot be used to unlock a device that has security technology like Touch ID enabled, and a passcode or password must be used instead. These circumstances may include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) five unsuccessful attempts to unlock the device via Touch ID are made; (4) when more than 48 hours has passed since the last time the device was unlocked; and (5) when the device has not been unlocked via Touch ID in eight hours and the passcode or password has not been entered in the last six days.

37. Similarly, in some circumstances, the user's face cannot be used to unlock a device that has security technology like Face ID enabled, and a passcode or password must be used instead. These circumstances may include: (1) the device has just been turned on or restarted; (2) the device has not been unlocked for more than 48 hours; (3) the passcode has not been used to unlock the device in the last 156 hours (six and a half days) and Face ID has not unlocked the device in the last four hours; (4) the device has received a remote lock command; (5) after five unsuccessful attempts to match a face; (6) after initiating power off/Emergency SOS by pressing

and holding either volume button and the side button simultaneously for two seconds. Thus, in the event law enforcement encounters a locked mobile device, the opportunity to unlock the device via fingerprint or face recognition exists only for a short time.

38. The passcodes or passwords that would unlock any smartphones seized in connection with this warrant are not known to law enforcement. Thus, it may be necessary to press the fingers of someone found in the Subject Premises, to any smartphones seized in connection with this warrant in an attempt to unlock the device(s) for the purpose of executing the search authorized by the warrant sought by this Affidavit. Similarly, it may be necessary to have someone found in the Subject Premises remain still and look, with eyes open, at the camera of any smartphones seized in connection with this warrant in an attempt to unlock the device(s) for the purpose of executing the search authorized by this warrant. Attempting to unlock any smartphones seized in connection with this warrant with the use of the user's fingerprints or face may be necessary because the Government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by the warrant being sought.

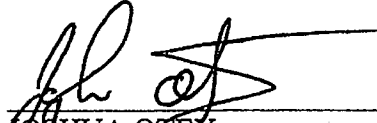
39. Although I do not know whether any smartphones will be seized in connection with this warrant or whether any fingerprints of anyone found in the Subject Premises will be capable of unlocking any of such devices, based on my training and experience I know that it is common for users to unlock their devices via the fingerprints on their thumbs or index fingers. In the event that law enforcement is unable to unlock any smartphones seized in connection with this warrant within the number of attempts permitted by the devices' security features, this will simply result in the devices requiring the entry of a password or passcode before it can be unlocked.

40. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of COOLIDGE to any smartphones seized in connection with this warrant, or

to instruct COOLIDGE to remain still, with eyes looking forward at the camera of any smartphones seized in connection with this warrant, for the purpose of attempting to unlock the devices in order to search the contents as authorized by the warrant sought by this Affidavit.


IV. Conclusion

41. Based on the foregoing, I respectfully request the court to issue a warrant to search the Subject Premises, described in Attachment A, and to seize and search the items described in Attachment B.



JOSHUA ONEY
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 9th day of August __, 2023



HONORABLE JUDGE KEVIN DOYLE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF VERMONT

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of VermontIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)81 BERLIN STREET, APARTMENT 2,
MONTPELIER, VT

Case No. 2:23-mj-098

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ Vermont
(identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B, incorporated herein describing evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A.

YOU ARE COMMANDED to execute this warrant on or before August 23, 2023 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Honorable Kevin J. Doyle, U.S. Magistrate Judge
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: August 9, 2023
5:27 p.m.City and state: Burlington, VermontKevin J. Doyle
Judge's signature
Honorable Kevin J. Doyle, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) is 81 Berlin Street, Apartment 2, Montpelier, Vermont. 81 Berlin St. is a two-story grey building with three apartment units. The Subject Premises is an apartment within the building having an entry at the rear of the 2nd floor of the building. Apartment 2 is the only apartment accessed from the rear of the building. 81 Berlin St. is shown in the following image taken on or about August 9, 2023:



ATTACHMENT B

I. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offense

The items to be seized from the Subject Premises are the following evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2251 (production of child pornography), 2252(a)(2) & 2252A(a)(2) (receipt of child pornography), and 2252(a)(4) & 2252A(a)(5) (possession of child pornography) (the "Subject Offense"):

1. Computer devices, storage media, cellular telephones, and related electronic equipment used to access, transmit, or store information relating to the Subject Offense;
2. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
3. Books and magazines containing visual or written depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
4. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
5. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
6. Correspondence and records pertaining to violation of the Subject Offense including, but not limited to envelopes, letters, mailings, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
7. Records evidencing occupancy or ownership of the Subject Premises, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence;
8. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the Subject Offense, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.
9. Information or correspondence pertaining to affiliation with any child exploitation bulletin boards, chat forums, or organizations;
10. Any child pornography as defined by 18 U.S.C. § 2256(8);

11. Any child erotica, defined as suggestive visual depictions of nude minors which do not constitute child pornography as defined by 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
12. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
13. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
14. Mailing lists, supplier lists, and mailing address labels related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2); and
15. Financial records, including credit card information, bills, and payment records related to related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises include any computer devices, storage media, and related electronic equipment that may contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offense falling within the categories set forth in Section I.A above. In lieu of seizing any such computer devices, storage media, and related electronic equipment, this warrant also authorizes their copying for later review.

To facilitate this review, the items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

3. Any records or other items which evidence ownership, control, or use of, or access to any seized or copied computer devices, storage media, and related electronic equipment, including but not limited to sales receipts, warranties, bills for internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs.

Any materials seized under this Section II.B that are later determined not to contain or constitute fruits, evidence, and/or instrumentalities of the Subject Offense falling within the categories set forth in Section II.A above will be returned to the Subject Premises within 60 days of their seizure.

C. Use of Fingerprints and Face

During the execution of this search warrant, law enforcement personnel are authorized to press the fingers (including thumbs) of COOLIDGE to the fingerprint sensor of any smartphones seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. During the execution of this search warrant, law enforcement personnel are authorized to have COOLIDGE remain still and look, with eyes open, at the camera of any smartphones seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.